ABSTRACT

A method and apparatus for protecting against a buffer over flow attack. In one variation, an executable software program is divided into an executable image, a data image, and an execution history image. The operating system processes an executable statement in the executable image. Other statements are processed in the data image. In a second variation, the execution history image is made use of in addition to the tasks of the first variation. Each statement is classified as either mutable or immutable. The usage of statements is recorded in the execution history image. If a mutable statement has over-written an immutable statement memory location, then the program is terminated. Optionally, the entire program is re-mapped using the execution history image such that immutable statements cannot over-write mutable statements.